Proof Theory in Bounded Arithmetic Systems(限定算術体系の証明論)

著者	多田 充
号	63
発行年	1997
URL	http://hdl.handle.net/10097/12750

氏　名（本　籍）	多田（ただ）　充（みつる）　（茨城県）
学位の種類	博士（情報科学）
学位記番号	情博第63号
学位授与年月日	平成10年3月25日
学位授与の要件	学位規則第4条第1項該当
研究科，専攻	東北大学大学院情報科学研究科（博士課程）情報基礎科学専攻
学位論文題目	Proof Theory in Bounded Arithmetic Systems （限定算術体系の証明論）
論文審査委員	（主査） 東北大学教授　静谷　啓樹　　東北大学教授　丸岡　章 東北大学教授　西関　隆夫　　東北大学助教授　満保　雅浩

論文内容要旨

限定算術の体系 S^i_2（$i \in \mathrm{N}$）は構造的計算量理論に対する証明論からのアプローチを可能とするものである。しかし S^0_2 の性質は十分に解明されておらず，解決すべき点が多い。本論文は体系 S^0_2 に関する新しい性質の証明，S^0_2 を拡張した体系である S^0_{2+} の一性質に関する従来の予想の肯定的解決，及び限定算術体系の応用として，現代暗号系の安全性の解析結果等の成果をとりまとめたもので，全編6章からなる。

1　はじめに

第1章は序論である。ここでは本研究についての背景，目的を述べている。S. Buss による限定算術の体系 S^i_2（$i \in \mathrm{N}$）は，計算量理論における多項式時間階層と密接な関係があることで大変興味を持たれている。その関係とは「$i \geq 1$ のとき，S^i_2 において Σ^b_i クラスで定義される関数のクラスと計算量理論におけるクラス $\mathrm{F}\Delta^p_i$ は一致する」というもので，$i=1$ を代入することにより，「S^1_2 において Σ^b_1 クラスで定義される関数のクラスと多項式時間で計算できる関数のクラス FP は一致する」ことが得られる。つまり，このことにより効率的な計算ができるかどうかを算術の側から考えることができるのである。

しかし，算術体系 S^0_2 と計算量のクラスとの関係については十分に解明されていない。S^0_2 の性質として，竹内外史［5］により減算が S^0_2 において定義できないことと，J. Johannsen［2］により3による除算が S^0_{2+} において定義できないことが知られている。そこで本論文では，算術体系 S^0_2 及び S^0_{2+} における「定数 m による除算」を考え，それらの体系で除算が定義できることの必要十分条件が「m が2の巾であること」であることを証明する。

また，S^1_2 と FP の関係の応用として，暗号理論において重要な役割を果たす素因数分解を限定算術の中で考える。ここでの素因数分解とは，「暗号システムを破る素因数分解」のことなので，この論文において素因数分解数とは，入力 a が二つの素数 p, q の積であるときに限り，その素数の組を出力するものとする。

2　準　備

第2章は準備の章である。ここでは本論文の研究対象となる算術体系 S^i_2 の定義と，その基本的な性質を与える。

算術体系 S^i_2 は，Gentzen の古典論理の体系 LK に関数記号と述語記号に関する公理と幾つかの推論規則を付け加えたものである。S^i_2 の言語は定数記号 0，関数記号 S, +, ・, $|*|$, $\lfloor */2 \rfloor$, #，述語記号 =, $\leq$，論理記号 $\wedge$, $\vee$, $\neg$,

つ, $\forall$, $\exists$ 及び補助記号（カッコとコンマ）から成る。ここで，関数記号 S は後者関数，$|*|$, $\#$ は $|x|=\lceil\log_2(x+1)\rceil$, $x\#y=2^{|x|\cdot|y|}$ をそれぞれ意味する。新しく付け加えられる推論規則は限定された束縛記号（$\forall x\leq t$），（$\exists x\leq t$）に関する規則と以下の帰納法規則 Σ_i^b-PIND である。

$$\frac{\Gamma, A(\lfloor a/2\rfloor) \longrightarrow A(a), \Delta}{\Gamma, A(0) \longrightarrow A(t), \Delta}$$

t は任意の項，a は自由変数で下式には現われないものとする。また，A はクラス Σ_i^b の式である。ここで，式のクラス Σ_i^b 及び Π_i^b は算術的階層 Σ_i, Π_i と同じように構成されるが，そこでは束縛記号（$\forall x\leq t$），（$\exists x\leq t$）が算術的階層における（$\forall x$），（$\exists x$）の役割をして，（$\forall x\leq|t|$），（$\exists x\leq|t|$）が算術的階層における（$\forall x\leq t$），（$\exists x\leq t$）の役割をする。限定されていない束縛記号（$\forall x$），（$\exists x$）が含まれる式は，どの Σ_i^b, Π_i^b にも属さない。算術体系 S_2^i の関数記号及び述語記号に関する公理は BASIC と呼ばれ，32の式から成り立ち，それらは関数及び述語記号の基本的な性質を表わすのに十分である。

「関数 f が体系 L においてクラス R で定義できる」とは次の式が L で証明でき，かつ式中の G_f がクラス R に属することとする。

$$(\forall x)(\exists!\, y\leq t)\, G_f(x,y)$$

このことを簡単に $D(f, L, R)$ と書くことにする。Buss によって $D(f, S_2^i, \Sigma_i^b) \Leftrightarrow f\in F\Delta_i^p$ となることが示されている。このとこから，$D(f, S_2^1, \Sigma_1^b) \Leftrightarrow f\in FP$ となることがわかる。$D(f, S_2^i, \Sigma_i^b)$ である関数の関数記号は S_2^i の証明の中で自由に使ってよい。

3　算術体系 S_2^0 の弱さ

第3章は算術体系 S_2^0 における除算の研究である。竹内外史［5］により，減算が S_2^0 では定義できないことが証明されているが，この章では同じ手法により「定数 m により除算が S_2^0 で定義できること」の必要十分条件が「m が2の巾であること」を証明する。

竹内外史［5］は，S_2 における S_2^0 の解釈として DS-version というものを定義している。それは，関数，項，式について帰納的に定義されている。定数0及び自然数 a は，それぞれ空列 $\langle\rangle$ 及び下降列 $\mathrm{Ds}(a)$（$=\langle a_1,\ldots,a_n\rangle$）として解釈される。ここで $a_1,\ldots,a_n$ は $a_1>\cdots>a_n$，$2^{a_1}+\ldots+2^{a_n}=a$ を満たす。A が下降列であることを $\mathrm{Dseq}(A)$ と書く。下降列 $\mathrm{Ds}(a)$ の要素の個数は a の二進表示したときの1の個数によってきまる。

関数 f の DS-version D^f とは次の可換図を満たす関数 g と定義する。

$$\begin{array}{ccc} a_1,\cdots,a_n & \xrightarrow{\ f\ } & f(a_1,\cdots,a_n) \\ \mathrm{Ds}\downarrow & & \downarrow\mathrm{Ds} \\ A_1,\cdots,A_n & \xrightarrow[\ g\ ]{} & g(A_1,\cdots,A_n) \end{array}$$

一般に g の定義は一意的ではないが，限定算術の初期関数の DS-version は全て，多項式時間で計算可能になるように定義できる。

項 t の DS-version t^{DS} は t が $0, a$ の形のときはそれぞれ $\langle\rangle$, $\mathrm{Ds}(a)$, $f(t_0)$ の形のときは $D^f(t_0^{DS})$, $g(t_1,t_2)$ の形のときは $D^g(t_1^{DS}, t_2^{DS})$ と帰納的に定義される。

原始式 $s=t, s\leq t$ の DS-version はそれぞれ $s^{DS}\overset{D}{=}t^{DS}$, $s^{DS}\overset{D}{\leq}t^{DS}$ と定義される。その意味はそれぞれ $\mathrm{Ds}^{-1}(s^{DS})=\mathrm{Ds}^{-1}(t^{DS})$, $\mathrm{Ds}^{-1}(s^{DS})\leq\mathrm{Ds}^{-1}(t^{DS})$ である。一般の式 φ の DS-version φ^{DS} は，原始式の DS-version から帰納的に定義される。

以上により S_2 における S_2^0 の解釈が与えられる。このとき竹内外史［5］により

$$S_2^0 \vdash \varphi(\boldsymbol{a}) \Rightarrow S_2 \vdash \mathrm{Dseq}\ (A) \supset \varphi^{\mathrm{DS}}\ (A)$$

が示されている。

今，式$\Theta_m(a, q)$を$m \cdot q \leq a < m \cdot S(q)$と定義する。定数$m$が2の巾のときには容易に$S_2^0 \vdash (\exists q)\Theta_m(a, q)$が示される。$m$が2の巾ではないときは，$\lfloor 2^a / m \rfloor$の商の二進表示における1の個数は$a$に比例するので，関数$\lfloor a / m \rfloor$のDS-version $D^{\lfloor * / m \rfloor}$は一般に値が大きすぎ，その値の存在は限定算術の範囲内では証明できない。以上により「$\mathrm{D}(\lfloor a / m \rfloor, S_2^0, \Sigma_1^b) \Leftrightarrow m$が2の巾」であることが証明される。

このことにより，その性質が殆ど知られていない算術体系S_2^0の一つの性質が明らかにされた。

4　拡張した算術体系 $S_2^0{}_+$

第4章はS_2^0を拡張した体系$S_2^0{}_-$に関する研究である。前章と[5]により，定数mが2の巾でないとき除算がS_2^0で定義できないことが示されたが，S_2^0に減算を付加すれば除算の条件にどういう影響があるかというのが研究の動機である。Johannsen[2]は，関数$\lfloor a / 3 \rfloor$が$S_2^0{}_+$で定義できないことを示し，その上「定数mが2の巾でないとき関数$\lfloor a / m \rfloor$が$S_2^0{}_-$で定義できない」ことを予想している。本論文では，この予想が正しいことを証明する。

$S_2^0{}_-$とは，S_2^0に減算を含む幾つかの関数記号とその関数の基本的な性質を表わす公理を付加した算術体系である。前章では，DS-versionによってS_2におけるS_2^0の解釈を与えたが，ここではJohannsen[2]によるCode-versionを用いてS_2における$S_2^0{}_-$の解釈を与える。

定数0及び自然数aは，それぞれ空列〈〉及び正列$\mathrm{Code}(a)$(=$\langle a_1, \ldots, a_n \rangle$)として解釈される。ここで$a_1, \ldots, a_n$は$a_1 > 0, \ldots, a_n > 0$を満たし，また$a$の二進表示は次のようになっているとする。

$$\underbrace{1\cdots1}_{a_1}\underbrace{0\cdots0}_{a_2}\cdots\underbrace{c\cdots c}_{a_n}$$

ここで$c \in \{0, 1\}$である。Aが正列であることを$\mathrm{PSeq}\ (A)$と書く。前章と違い，正列$\mathrm{Code}\ (a)$の要素の個数はaの二進表示したときの1と0の交代の回数によってきまる。

Code-versionは，関数，項，式について定義され，その定義はDS-versionの場合と全く同様である。

このようにしてS_2における$S_2^0{}_-$の解釈が与えられる。このときJohannsen[2]により

$$S_2^0{}_- \vdash \varphi\ (\boldsymbol{a}) \Rightarrow S_2 \vdash \mathrm{PSeq}\ (A) \supset \varphi^C\ (A)$$

が示される。

算術体系$S_2^0{}_-$はS_2^0により明らかに強いので，定数mが2の巾の場合は同様にして$(\exists q)\Theta_m(a, q)$が$S_2^0{}_-$で証明できることがわかる。減算では入力$a, b$の差における1と0の交代の回数は，$a, b$のそれと殆ど変わらないのに対して，除算では$m$が2の巾ではないときは，$\lfloor 2^a / m \rfloor$の商の交代の回数はやはり$a$に比例するので，関数$\lfloor a / m \rfloor$のCode-version $C^{\lfloor * / m \rfloor}$は一般に値が大きすぎ，その値の存在は限定算術の範囲内では証明できない。以上により「$\mathrm{D}(\lfloor a / m \rfloor, S_2^0{}_-, \Sigma_1^b) \Leftrightarrow m$が2の巾」であることが証明される。

このことにより，算術体系S_2^0に減算を付加しても除算が定義できるための条件は全く変わらないことがわかり，Johannsenの予想が正しいことがわかる。

5　限定算術の暗号理論への応用

第5章では暗号理論を限定算術の側から考えている。現在使われている暗号系の多くは，素因数分解問題と離散対数問題の難しさを利用している。ここでは素因数分解問題に焦点を当てている。RSA等の暗号系は素因数分解が一般に難しいという仮定でもって，その安全性が保障されているのだが，その仮定は単に「素因数分解の効率的な解法が発見されていないこと」にすぎない。故に，多項式時間で計算できる素因数分解の方法が構成できればそれらの暗号系はもはや安全ではなくなる。本論文では「$\mathrm{D}(f, S_2^1, \Sigma_1^b) \Leftrightarrow f \in \mathrm{FP}$」という事実を考慮し，素因数分解関数Factを$S_2^1$において$\Sigma_1^b$で定義することを考える。

Prime(a)を一般に知られている素数のco-NP-定義，つまり

$$(\forall p, q < a)\,[\,a = pq \supset (p = 1 \vee q = 1)\,]$$

とする。この式は Π_1^b に属すが，その排中律はクラス $\Sigma_2^b \cap \Pi_2^b$ に属す。これは Σ_1^b より大きいクラスなので，このままでは $D(\mathrm{Fact}, S_2^1, \Sigma_1^b)$ とはならない。そこで，Pratt [4] による素数の NP-定義 Pratt (a) を用いて素因数分解関数を定義する。

$$(\forall x)\,[\,\mathrm{Prime}\,(x) \supset \mathrm{Pratt}\,(x)\,]$$

という式を Ψ で表わす。Krajíček により素因数分解関数の一意性が示されており，また本論文により素因数分解関数の値の存在が $S_2^1 + \Psi$ で証明されるので，$D(\mathrm{Fact}, S_2^1 + \Psi, \Sigma_1^b)$ であることがわかる。Fact が FP に属すためには S_2^1 において Ψ が証明されなければならないが，それはかなり困難であると予想される。なぜなら Pratt による「素数判定問題が NP∩co-NP に属す」ことの証明には，多項式時間で計算できるかどうかわからない関数が現われるのに対し，S_2^1 で使用できる関数記号はクラス FP のものに限られているからである。

以上により素因数分解の難しさの一面が示され，多くの暗号系の安全性の一つの拠り所が与えられた。

6 まとめ

第6章では結論とともに，今後の課題となりうる題材を述べている。

参考文献

[1] S. R. Buss : Bounded arithmetic, Bibliopolis, Napoli, 1986.

[2] J. Johannsen : "On the weakness of sharply bounded polynomial induction", A. Leitsch and D. Mundici (eds.), Computational Logic and Proof Theory, volume 713 of Lecture Notes in Computer Science, pp. 223-230, Springer-Verlag, 1993.

[3] J. Krajíček and P. Pudlák : "Some consequences of cryptographical conjectures for S_2^1 and EF", D. Leivant (ed.), Logic and Computational Complexity, volume 960 of Lecture Notes in Computer Science, pp. 210-220, Springer-Verlag, 1994.

[4] C. H. Papadimitriou : Computational Complexity, Addison-Wesley Publishing Company, 1994.

[5] G. Takeuti : "Sharply bounded arithmetic and function $a \dot{-} 1$ " W. Sieg (ed.), Logic and Computation, Contemporary Mathematics 106, pp. 281-288, 1990.

審 査 結 果 の 要 旨

計算量のクラスの包含関係を明らかにする問題は構造的計算量理論の中心的問題であり，証明論の立場からは，限定算術体系を用いてこの問題を解明することが試みられている。S^1_2 と呼ばれる限定算術体系は，多項式時間階層との密接な対応関係が示されており，限定算術体系のなかでも最も重要な体系であるが，その性質は十分には解明されていない。

著者は，体系 S^1_2 に関する新しい性質を証明し，S^1_2 を拡張した体系である $S^1_{2^-}$ に関する従来の予想を肯定的に解決し，さらに限定算術体系を応用して，現代暗号系の安全性を解析した。本論文はこれらの成果をとりまとめたもので，全編6章からなる。

第1章は序論である。

第2章では，研究の背景として，限定算術体系に関する一般的事項を紹介している。

第3章では，体系 S^1_2 における算術演算の制限に関して考察し，S^1_2 においては，2のべき乗で表される自然数以外での除算は，関数として定義不可能であることを証明している。これは，初めて明らかにされた S^1_2 に関する性質であり，証明論における重要な成果である。

第4章では，S^1_2 にいくつかの公理を追加した拡張体系である $S^1_{2^-}$ の性質を考察し，この体系においては，2のべき乗で表される自然数以外での除算は不可能であろうという従来の予想が正しいことを証明している。これは，重要な知見である。

第5章では，限定算術体系の応用として，素因数分解問題の困難さに基づく暗号系の安全性を考察し，体系 S^1_2 では証明できないと予想されている公理を S^1_2 に付加すると，素因数分解問題が多項式時間で解けてしまうことを証明している。これは，現代暗号系の安全性に関する一つの拠りどころを与えているものであり，暗号理論上高く評価できる。

第6章は結論である。

以上要するに本論文は，限定算術体系の性質に関する未知の事実を明らかにするとともに，現代暗号系の安全性解析に限定算術体系を応用する一手法も与えたものであり，理論計算機科学及び情報基礎科学の発展に寄与するところが少なくない。

よって，本論文は博士（情報科学）の学位論文として合格と認める。